

## CS3670-2 Secure Management of Systems (3-2) Fall 2003

This course provides students with an understanding of management concerns associated with the security of computer-based information systems. In particular, students will examine both the technical and non-technical security issues associated with managing a computer facility, with emphasis on DoD computer systems and policies. Laboratory exercises will be used to demonstrate specific skills or tools that can be used to defend computer systems. **PREREQUISITE:** CS3600.

Course Hours		Instructor
Lecture:	SP 231, 1400 (M, Tu, W)	Paul Clark
Laboratory:	SP 511, 0900-1050 (F)	Office: Sp 532A
		Email: <a href="mailto:pcclark@nps.navy.mil">pcclark@nps.navy.mil</a>
		Office Phone: 656-2395

<http://www.cs.nps.navy.mil/people/faculty/clarkp>

### Texts

Lecture Slides (available in the bookstore)  
No other textbook is required.

### Topics Covered

Security Plan	Technical Protection	Contingency Planning
Security on the OS	Current Legal issues	Physical Security
Professional Certifications	Policies, Standards, etc.	

### Grading

Exam #1:	20%	Grading will be assigned on a straight point system:		
Exam #2:	20%	A 96-100	B 84-87	C 72-75
Homework:	10%	A- 91-95	B- 80-83	C- 68-71
Labs	10%	B+ 88-90	C+ 76-79	D 64-67
Security Plan	20%			
Group Project	15%			
Class Participation and professionalism	5%			

Current estimated test dates: Nov 5<sup>th</sup>, Dec 10<sup>th</sup>.

(over)

## Policies

1. Assigned work is due at the beginning of class. Otherwise, it is considered late, and given a lower score. Late work is only acceptable if arrangements are made in advance. This means that **if you are officially in the first section, then you are expected to turn in the assignment at the beginning of the first section**, not the beginning of the second session.
2. Assigned work is to be done individually, unless it is an assigned group project.
3. Plagiarism is unacceptable. No “gouge” is allowed for assigned work. For example, answers to assignments are not to be copied from someone who did them in a previous quarter. Quoting from other sources must be cited, including lecture notes. Violating this policy will result in consequences ranging from a lower grade on the affected assignment to notification of the curricular officer. I should therefore never see two papers that are almost word for word identical, unless those duplicate words are cited in both papers.
4. Using a “gouge” to study for a test is allowed. However, the tests are closed book.

## Lab Assignments (Done in Pairs)

Install Windows XP (and secure it)  
Install Linux (and secure it)  
Unix Tutorial  
Vulnerability Scanning  
Forensic Exercise  
Other exercises as time, resources and imagination allow.

## Projects

### Project #1 (Group Project)

An (intended) quarter-long project that looks into various aspects of security. These will be projects unique to each group. Groups can range from two to four people, depending on the difficulty of the task.

Deliverables:

1. A written report.
2. A 20-minute class presentation somewhere between weeks 8 and 11.

### Project #2 (Individual Project):

Given a description of a computer facility, develop a security plan for it. Identify the current security problems and present a plan for improvement.

Deliverable: A written report.